

EXPRESS MAIL LABEL NO.: EL395555156US DATE OF DEPOSIT: January 10, 2001

I hereby certify that this paper and/or fee are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR §1.10 on the date indicated above and is addressed to the Assistant Commissioner of Patents, Washington, D.C. 20231.

Karen Roper
Karen Roper

**LAWFUL COMMUNICATION INTERCEPTION -
INTERCEPTING COMMUNICATION ASSOCIATED INFORMATION**

Inventor(s): Ronald D. Ryan
200 Diamond Ridge Drive
Coppell, Texas 75019
Nationality: U.S.A.

Fereidoun Homayoun
2805 Covey Place
Plano, Texas 75093
Nationality: Canada

Assignee: Nortel Networks Limited
380 St. Antoine Street West, 8th Floor
Montreal, Quebec H2Y 3Y4
Canada

Carr & Storm, L.L.P.
670 Founders Square
900 Jackson Street
Dallas, Texas 75202

**LAWFUL COMMUNICATION INTERCEPTION -
INTERCEPTING COMMUNICATION ASSOCIATED INFORMATION**

TECHNICAL FIELD

The invention relates generally to providing Law Enforcement Agencies (LEAs) with communication associated information (CAI), and, more particularly, to providing an efficient method and apparatus for extracting CAI for use by LEAs.

0957904-01004
F09F19-40625259

BACKGROUND

LEAs are allowed to partake in communications surveillance between a subject and an associate in an attempt to obtain further evidence of criminal activity. The evidence that the LEAs have historically been allowed to capture generally comprises call identifying information and call content of voice calls. Call identifying information generally comprises the calling party number and the called party number. Court orders allowing access to the call identifying information generally comprise a Trap-and-Trace order and a Pen Register order, and generally require only a suspicion of wrongdoing. Trap-and-Trace orders allow LEAs access to call identifying information for incoming calls placed to a specified device identified by a phone number, and Pen Register orders allow LEAs access to call identifying information for outgoing calls originating from a specified device or phone number.

Call content generally comprises the content of the call, such as the voice transmissions. Call content orders, commonly known as Title III orders, generally require proof that the subject of the order is engaging in, or there is a high likelihood that the subject of the order is about to engage in, illegal activity. It is estimated that about 10% of the orders are Title III orders, the remaining 90% comprising Trap-and-Trace orders and Pen Register orders.

The technological advances in the area of telecommunications, such as packet-switched networks, however, have provided additional methods and types of communication that render call identifying information less meaningful and difficult to obtain. As a result, the concept of a call,

which typically refers to a voice call, is generally replaced with the concept of a communication, which encompasses additional types of communications such as e-mail, Voice over Internet Protocol (VoIP), on-line banking, video, data of various types, and the like.

Communications generally comprise communication associated information (CAI) and communication content. CAI generally comprises communication identifying information, such as Internet Protocol (IP) addresses and session identifiers, call identifying information, call redirection commands, e-mail addresses, and the like. Communication content comprises the information exchanged between the subject and the associate, such as voice transmissions, text messages, credit card numbers, bank accounts, and the like.

Furthermore, in a packet-switched network, such as the Internet, a single message is generally broken into many packets, each packet containing routing information. The packets are sent through an access network, such as the Public Switched Telephone Network (PSTN), and re-assembled at the termination point. Since packet-switched communications are broken into many packets, an access network performing Trap-and-Trace and/or Pen Register orders would typically capture and report information for each packet, yielding voluminous CAI records for each communication sent and/or received by a subject.

The packets are generally organized according to the Open Standards Interconnect (OSI) seven-layer protocol model. The access networks generally route the packets of communication by evaluating the Network Layer 3, with the Layers 4-7, which typically contain the CAI and the communication content,

remaining unevaluated by the access networks. The Network Layer 3 of each packet generally comprises the routing information, which can also be considered CAI, such as the IP addresses of the source and destination network components for the packets. Therefore, communications sent or received via a service provider, such as America Online, generally comprise the IP addresses of the service provider and the subject. For some applications, the identifying information of the other party, i.e., the associate, is provided in the Application Layer 7.

For instance, e-mail service providers generally use the Application Layer 7 to communicate the addressee of an e-mail. When a subject sends an e-mail to an associate, the Network Layer 3 source and destination IP addresses comprise the IP addresses of the subject and the e-mail Service Provider. The e-mail address of the associate is generally placed in the Application Layer 7 by the e-mail application and, therefore, is generally not available to the access networks since the access networks evaluate the Network Layer 3. Moreover, for the access networks to evaluate the additional layers, there is a need for an indication of the application type allowing the access networks to isolate and send the CAI to the LEAs for Trap and Trace and Pen Register court orders.

Prior attempts at providing the necessary information have used applications that search packets for the necessary information, commonly referred to as "sniffers". Sniffers typically provide LEAs access to the entire communication. The LEAs then evaluate and remove the allowed material, such as the CAI. Access by LEAs to the entire communication,

however, violates the privacy of the individual absent a Title III content order.

Therefore, for these and other reasons, there is a need for a method allowing the access networks to isolate and
5 extract CAI of packet-based communications. Additionally, there is a need to provide CAI information obtained in a packet-based network in a condensed format.

09757504 041004

SUMMARY

The present invention provides a method and apparatus for providing LEAs with CAI for subjects of Trap-and-Trace and/or Pen Register surveillance orders. The method and apparatus
5 comprises populating the Network Layer 3 with an Application Identifier (AID), which the access networks use to isolate and extract CAI from the packet.

2025 RELEASE UNDER E.O. 14176

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the accompanying drawings, in which:

FIGURE 1 schematically depicts the typical network environment that embodies the present invention;

FIGURE 2 is a message format illustrating one embodiment in which the Network Layer 3 is populated with an application identifier tag (AID-tag) and an application identifier (AID);

FIGURE 3 is a message format illustrating another embodiment in which the Network Layer 3 is populated with an AID; and

FIGURE 4 is a flow chart illustrating one embodiment of consolidating and reporting CAI to the LEAs.

DETAILED DESCRIPTION

The principles of the present invention and their advantages are best understood by referring to the illustrated embodiment depicted in FIGURES 1-4.

5 Referring to FIGURE 1 of the drawings, the reference numeral 100 generally designates a communication system that embodies features of the present invention. The subject of the surveillance order 110 is connected to the access network 112 via a subject device 114, such as wireline phone, wireless
10 phone, laptop computer, desktop computer, Personal Data Assistant (PDA), and the like. The access network 112, such as the Public Switched Telephone Network (PSTN), a wireless communications network, the Internet, and the like, provides communications services between the subject 110 and the
15 associate 116. The associate 116 accesses the communications via an associate device 118, such as a wireline phone, wireless phone, laptop computer, desktop computer, PDA, and the like. Moreover, a service provider and/or intermediary 120, such as America On-Line, Microsoft Network, and the like,
20 generally provides communication services, such as e-mail, Voice-Over-IP (VoIP), video conferencing, banking, and the like. The details of the subject device 114, the associate device 118, the access network 112, and the service provider 120 are well-known to a person of ordinary skill in the art
25 and, therefore, will not be discussed in further detail. Furthermore, while only a single service provider 120 and associate 116 is shown, it is well-known to a person of ordinary skill in the art that each of these may be comprised of one or more and that the techniques disclosed in the
30 present application are equally applicable to each.

Communications from the subject 110 to the associate 116 typically involve information packets sent from the subject 110 to the service provider 120 via the access network 112. The service provider 120 then forwards the communication to the associate 116 via the access network 112. The access network 112 comprises an Intercept Access Point (IAP) 122 for the interception of the CAI and the call content for communications to and/or from the subject 110. The process of intercepting communications to and/or from a subject is well-known in the art and, therefore, will not be discussed in further detail.

Since the access network 112 and the IAP 122 are generally responsible for evaluating only the Network Layer 3, the preferred embodiment of the present invention inserts additional information into the Network Layer 3, allowing for the isolation and extraction of the CAI, as illustrated by the protocol stack in FIGURE 2. Generally, the protocol stack comprises the Network Layer 3 202 and the Application Layer 7 204. The remaining layers, the Physical Layer 1 205, the Data Link Layer 2 206, the Transport Layer 4 207, the Session Layer 5 208, and the Presentation Layer 6 209 are shown for completeness and are well known to one of ordinary skill in the art and, therefore, will not be discussed in greater detail.

The Network Layer 3 202 generally comprises a source IP address 210, a destination IP address 212, the User Datagram/Transmission Control Protocol field 214, a protocol field 216, and optional data fields 218. Preferably, the protocol field 216 comprises an application identifier tag (AID-tag) 217, such as a code of 99, that indicates an

optional data field 218 is present comprising an application identifier (AID) 220. The AID 220 preferably comprises a unique identifier for a vendor and/or application, such as Microsoft Outlook, Netscape Mail, and the like. Given the AID 220, the format of the CAI 222 included in the Application Layer 7 is known to the access network, and the CAI 222 can be extracted and reported to the LEAs in a meaningful format.

In operation, a known AID-tag 217, such as 99, indicates that the packet includes an optional field, which includes an AID 220 that indicates the packet was sent by a specific vendor and/or application. Since the vendor and/or application is known, the format of the CAI included in the Application Layer 7 is known, and the CAI may be extracted and reported to the LEAs.

The values and the meanings of the protocol field 216 are generally governed by a standards organization, such as the Internet Engineering Task Force (IETF). Therefore, for every value the LEAs request to be assigned to the protocol field 216, the LEAs must work with the IETF and members of the industry to have the value assigned. Additionally, the protocol field 216 is typically limited to an 8-bit field, limiting the number of values available to the LEAs and hence the number of vendor/application pairs that may be identified.

The optional field 218, however, neither requires the interaction with the standards organizations nor is it subject to the 8-bit size limitation. Therefore, by placing the AID 220 in the optional field 218, the AID 220 can be assigned a greater range of values without the need of approval from a standards. The LEAs and the members of the industry only

require one value to be assigned for the AID-tag 217 in the protocol field 216.

Alternatively, the protocol stack comprises a structure as illustrated in FIGURE 3. In this instance, the protocol field 216 comprises an AID 220 indicating a vendor and/or an application, such as the Microsoft Outlook e-mail application. While this embodiment is subject to the size and allocation limitations discussed above, this embodiment presents significant advantages over the prior art by allowing the access networks to isolate, extract, and report the CAI.

Referring back to FIGURE 1, the IAP intercepts communications to and/or from the subject 110 and routes the packets to a distributor 130. The distributor 130 routes the packet to an Application CAI Isolator 132 corresponding to the AID 220 extracted above. The Application CAI Isolator 132 parses the Application Layer 7 204, extracting the CAI 222. The CAI 222 is then sent to a delivery function 134 that consolidates and delivers the CAI 222 to the appropriate LEA 136.

In operation, the IAP 122 intercepts packets sent to and/or from the subject 110 containing an AID-tag 217 and/or an AID 220 that indicates the packet contains CAI 222. The distributor 130 evaluates the AID 220 and routes the packet to the appropriate Application CAI Isolator 132. The Application CAI Isolator identifies the format of the Application Layer 7 204 and extracts the CAI 222. The CAI 222 is extracted and sent to the delivery function 134 for consolidation and reporting to the LEAs.

The process of delivering and consolidating is further illustrated in FIGURE 4. In step 410, the CAI 222 that was

either sent to and/or by the subject is received by the delivery function 134. The delivery function 134 first determines whether the CAI 222 is a known CAI, i.e. a first instance of the CAI, as in step 412. A list of active CAI is maintained in a list KNOWN_CAI. As CAI is received, the CAI is compared to the list KNOWN_CAI. If the CAI is not in KNOWN_CAI, the CAI is preferably treated as a new instance of a CAI of the communication between the subject and the associate. If the CAI is in KNOWN_CAI, however, the CAI is preferably treated as a CAI of an ongoing communication. Moreover, for each instance of CAI, a CAI_COUNTER and a 1st_INSTANCE_FLAG is maintained. The CAI_COUNTER indicates the number of packets identified by the CAI that have been sent and/or received by the subject. The 1st_INSTANCE_FLAG indicates whether the CAI is a new instance of a CAI.

If the CAI received is a new instance of a CAI, the CAI is added to the list KNOWN_CAI, a CAI_COUNTER is initialized, and a 1st_INSTANCE_FLAG is set, as in step 414. Thereafter, in step 416 the CAI_TIMER is set to initialize a timeout counter, such as two minutes and the like, in step 418 a message comprising the CAI is sent to the LEAs with the 1st_INSTANCE_FLAG set and the CAI_COUNTER, and in step 420 the 1st_INSTANCE_FLAG is cleared and the CAI_COUNTER is reset.

The message preferably comprises a subject identifier, a time stamp indicating when the message was sent and/or received, the IP address of the subject 110, a packet direction indicator identifying whether the message was sent or received by the subject 110, the IP address of the associate, a first instance indicator identifying the a new instance of a CAI, and a CAI counter indicating the number of

packets identified by the CAI seen since the last report. As the law develops and allows the LEAs access to additional information, additional fields may be extracted from the CAI and reported to the LEAs.

5 If the packet received is not a new instance of a CAI in step 412, the CAI_COUNTER is incremented and the CAI_TIMER is set to indicate the receipt of an additional packet identified by the CAI, as in step 422. This process of counting the number of packets identified by the CAI received without
10 sending a message to the LEAs will continue until the CAI_COUNTER is equal to an adjustable THRESHOLD_COUNT, as in step 424. When the CAI_COUNTER equals the THRESHOLD_COUNT, the message will be sent and the CAI_COUNTER will be reset as in steps 418 and 420. Otherwise, no message will be sent, as
15 indicated by step 424. Thereafter, the delivery function awaits the receipt of CAI or the expiration of the CAI_TIMER, as in step 425.

 Additionally, processing will occur when the CAI_TIMER expires, as indicated in step 430. When the timer expires,
20 the delivery function 134 determines whether the CAI_COUNTER is equal to zero, indicating that a packet identified by the CAI has not been received in a predetermined amount of time and the number of packets identified by the CAI received has yet to be sent. In this case, the CAI_TIMER is set, as in
25 step 416, a message is sent with the current CAI_COUNTER, as in step 418, and the CAI_COUNTER is reset to zero, as in step 420.

 Since the CAI_TIMER has been set in step 416, the timer will expire and the delivery function 134 will begin
30 processing again at step 430 if no additional CAI are

received. This time, however, the CAI_COUNTER will equal zero in step 432. As a result, the CAI_TIMER will be cleared in step 434 and a CAI message with a CAI_COUNTER of zero will be sent. Thereafter, the delivery function 134 awaits the arrival of CAI, as in step 425.

It is understood that the present invention can take many forms and embodiments. Accordingly, several variations may be made in the foregoing without departing from the spirit or the scope of the invention.

Having thus described the present invention by reference to certain of its preferred embodiments, it is noted that the embodiments disclosed are illustrative rather than limiting in nature and that a wide range of variations, modifications, changes, and substitutions are contemplated in the foregoing disclosure and, in some instances, some features of the present invention may be employed without a corresponding use of the other features. Many such variations and modifications may be considered obvious and desirable by those skilled in the art based upon a review of the foregoing description of preferred embodiments. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.